Matt Bryant

https://programsareproofs.com

mbryant@programsareproofs.com
+1 412 737 3683

Overview

A software engineer with significant experience in **security**, **low-level systems**, and **performance**, with experience leading teams and a history of designing and implementing novel solutions to difficult problems.

Experience

Staff Engineer, Security at Asana — January 2019 – May 2025

Founded the Infrastructure Security team and served as its tech lead, preventing malicious actors from gaining access to customer data. My team ensured Asana shipped simpler and more robust infrastructure and guided other teams to analyze and prioritize security for new features.

In an IC capacity, I developed core infrastructure and led company-wide security culture and architecture:

- Responsible for the security architecture of Asana's wholesale infrastructure migration to Kubernetes, a multi-year project staffed by the entire Infrastructure department. Designed and implemented security controls to make it easier for engineers to build and maintain services while increasing their security.
- Implemented a custom network egress filter for all production traffic (>100GB/min), significantly raising the bar for attackers to exfiltrate data from and move laterally within Asana's infrastructure.
- Enforced mandatory code review for the entire company. Worked with dozens of teams across the org to demonstrate the policy's value and implement it without negatively impacting developer velocity.
- Introduced a programmatic data classification system for Asana's core data model, allowing developers to confidently work with data without risk of unintentionally exposing user content.
- Saved thousands of developer hours and millions of dollars of AWS spend yearly by optimizing various systems owned by teams including data science, CI/CD, developer experience, and core infrastructure.

Accomplishments: Led numerous projects that significantly elevated Asana's security posture. Shifted the conversation in the Infrastructure org to consider compartmentalization as table-stakes for new designs.

Software Development Engineer at Green Hills Software — July 2016 – January 2019

Worked on safety and performance critical code used around the world, particularly in hypervisors. Wrote code that secures everything from millions of cars to critical systems for several governments.

Accomplishments: Designed the world's highest-throughput mutex, developed a secure and high-performance GPU virtualization approach, ported a commercial operating system to Intel Skylake chips, and led a team building secure systems using hypervisors and separation kernels.

Security Research Intern at BAE Systems Applied Intelligence — June 2015 – August 2015

Researched efficient and non-invasive taint analysis for zero-day detection and analysis of common off-the-shelf programs, such a Microsoft Word.

Accomplishments: Designed a state-of-the-art scalable lock-free resizing hashtable, developed a 64-bit programmatic debugger, and contributed to a lock-free Python interpreter.

Security Intern at SilverSky — June 2014 – August 2014

Researched and built a novel system that successfully detected file-based zero-day exploits in commonly exploited programs, such as Internet Explorer and Microsoft Word, through server-side monitoring and behavioural analysis.

Teaching Assistant at Carnegie Mellon University — August 2013 – May 2016

Teaching assistant for six semesters at CMU, including for 15-410 (*Operating Systems Design*) and 15-411 (*Compiler Design*).

Software Engineer Intern at SilverSky — June 2013 – August 2013

Software Engineer Intern at Perimeter E-Security — June 2011 – August 2012

Education

Carnegie Mellon University — August 2012 – May 2016

Bachelor of Science in **Computer Science**, Minor in Mathematics

Projects

FunctionTrace (https://functiontrace.com)

Developed FunctionTrace, a low-overhead profiler for Python that provides a clear view of everything an application is doing. FunctionTrace is used by developers across the globe and was featured by Mozilla.

Languages and Tools

Significant professional experience developing in **Rust**, **Python**, **Terraform**, and **C**, and deploying with and securing **AWS** and **Kubernetes**. Working knowledge of **JavaScript**, **Go**, **x64 assembly**, **SQL**, **Bash**, and **OCaml**. Accustomed to working in and securing large and diverse codebases, ranging from webapps to operating systems.

Experience uncovering and debugging issues by whatever means necessary, including traditional debuggers (GDB, etc), Valgrind, disassembly, and unique hardware-based approaches.